

Step by Step Azure Site to Site VPN with SonicWall Hardware Firewall

Hussain Shakir

LinkedIn: <https://www.linkedin.com/in/mrhussain>

Twitter: https://twitter.com/hshakir_ms

Blog: <http://mstechguru.blogspot.com/>

Table of Contents

About Author	3
LAB Setup for Azure VPN.....	4
Requirements.....	4
Creating a virtual network	4
Creating Virtual Network Gateway.....	7
Creating Public IP Address	11
Define Gateway Subnet	12
Dashboard Status of Virtual Network Gateway.....	13
Property of Virtual Network Gateway	14
Insides of Virtual Network Gateway	15
Creating Connection Under Virtual Network Gateway	16
Creating an Address Object for the virtual network.....	17
SonicWall VPN Connection Creation.....	18
Testing the connectivity	24

About Author

Shakir is IT Consultant with over 13 years of extensive experience working with Microsoft Technologies AD, Exchange, O365, Windows Azure, PowerShell, Skype for Business, SQL, SharePoint and Microsoft public clouds, and providing solutions to different local & international Enterprise customers.

Shakir has been involved in Infrastructure Designing and Implementation, Virtualization, and Disaster Recovery. Extensive hands-on experience in Core Server Infrastructure, Cloud Computing, Virtualization/ Management and Information Protection. Analysis and Support of Microsoft Windows Server based Client / Server network, AD, Messaging, Skype for Business, SQL Always ON, Virtualization and System Center Infrastructure Products. Shakir has various industry certifications: MCT, MCTS, MCITP, MCSA, MCSE: Messaging, MCPS, MCSE: Cloud Platform and Infrastructure and also providing trainings on Microsoft Based Technologies.

LAB Setup for Azure VPN

Azure is a cloud computing platform and infrastructure created by Microsoft. It is used for building, deploying, and managing applications and services through a global network of Microsoft managed datacenters. For SonicOS platforms, Azure provides site-to-site Virtual Private Network (VPN) connectivity between a SonicWALL Next-Generation firewall and virtual networks hosted in the Azure cloud. In this Lab, we will walk through the requirement and step by step configuration with SonicWall 6600 with Site to Site VPN scenario.

Requirements

For setting up Site to Site VPN you need the followings: -

- Azure valid subscription
- SonicWall hardware.
- Valid Public IP Address at on premises side.

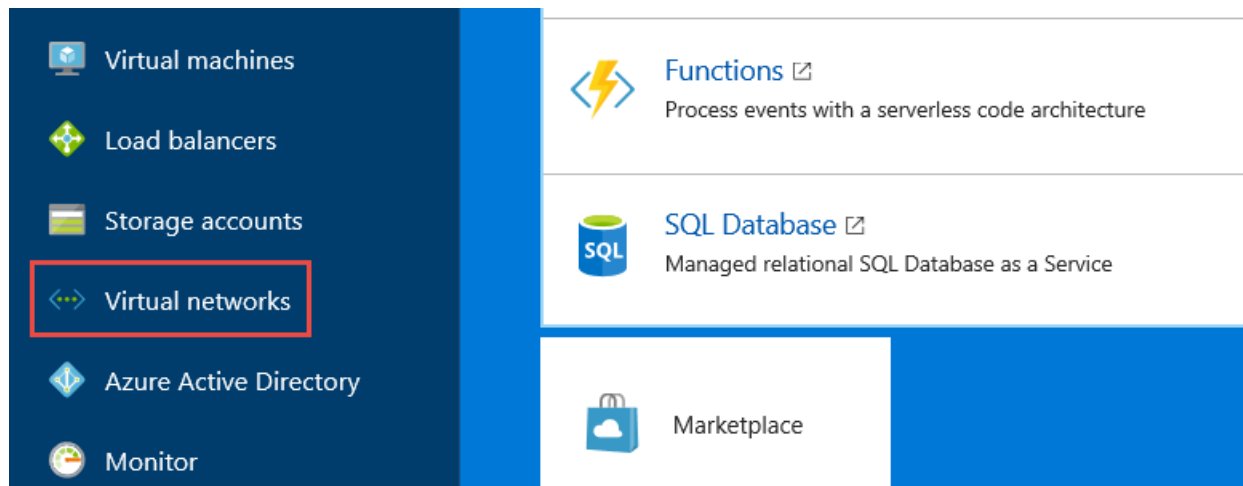
In my lab, I am going to use SonicWall Network Security Appliance (NSA) 6600 NGFW as its available in my network, you can use any low model SonicWall or any TZ series of the SonicOS.

Creating a virtual network

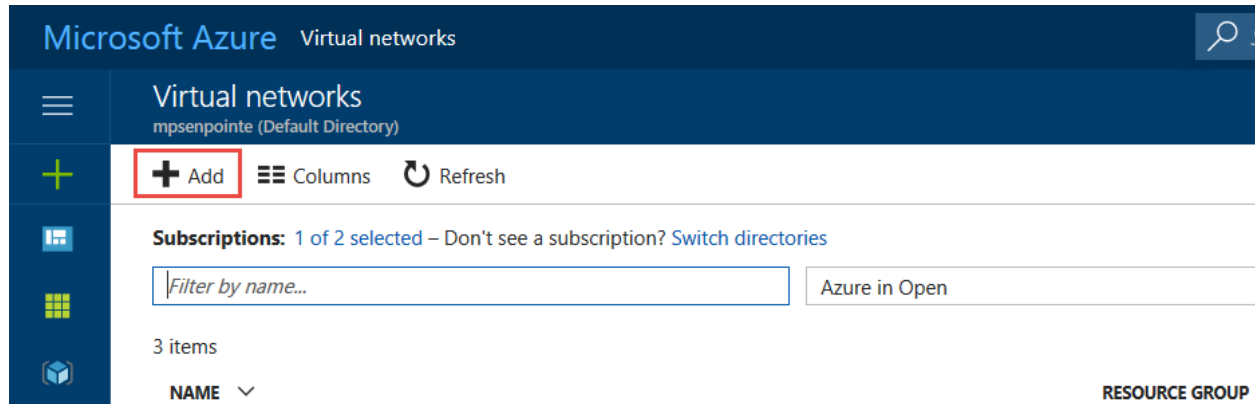
To create a virtual network through the Microsoft Azure Management Portal:

- Log into the Microsoft Azure Management Portal.
- In the left navigation menu, click Virtual Networks

You can also search by click New and search Virtual Network.



Click on +Add



Fill out the required information such as Name of the Virtual Network, Subnets, and Resource Group.

Create virtual network



* Name

SonicWall-Azure-Site2-Site-VPN-LAB



* Address space ⓘ

10.2.0.0/16



10.2.0.0 - 10.2.255.255 (65536 addresses)

* Subnet name

default

* Subnet address range ⓘ

10.2.2.0/24



10.2.2.0 - 10.2.2.255 (256 addresses)

* Subscription

Azure in Open



* Resource group ⓘ

☒ Create new ☐ Use existing

SonicWall-Azure-Site2-Site-VPN-LAB



* Location

Southeast Asia



☐ Pin to dashboard

Create

[Automation options](#)

Virtual networks		
mpsenpointe (Default Directory)		
<div> <div>+</div> Add <div>≡</div> Columns <div>↺</div> Refresh </div>		
Subscriptions: 1 of 2 selected – Don't see a subscription? Switch directories		
Filter by name...	Azure in Open	All locations
4 items		
NAME	RESOURCE GROUP	LOCATION
<--> [REDACTED]	[REDACTED]	Southeast Asia
<--> [REDACTED]	[REDACTED]	Southeast Asia
<--> SonicWall-Azure-Site2-Site-VPN-LAB	SonicWall-Azure-Site2-Site-VPN-LAB	Southeast Asia
<--> [REDACTED]	[REDACTED]	Southeast Asia





At this point we have successfully created virtual network, let's create Virtual Network Gateway for newly created virtual network.

Creating Virtual Network Gateway

Click New and search Virtual Network Gateway







Everything		
Filter		
<div> <div>🔍</div> Virtual Network Gateway </div>		
Results		
NAME	PUBLISHER	CATEGORY
<--> Virtual network gateway	Microsoft	Networking
<--> Local network gateway	Microsoft	Networking

Click Create

 Virtual network gateway   
Microsoft

A virtual network gateway is the software VPN device for your Azure virtual network. Use this with a [connection](#) to set up a site-to-site VPN connection between an Azure virtual network and your local network, or a VNet-to-VNet VPN connection between two Azure virtual networks. It can also be used to connect a virtual network to an ExpressRoute circuit.

Microsoft Azure provides a [99.9% uptime SLA](#) for virtual network gateways.

PUBLISHER	Microsoft
USEFUL LINKS	Service overview Documentation Pricing details

Create

Create virtual network gate...

×

* Name

VNG-4-SonicWall-VPN

✓

Gateway type ⓘ

VPNExpressRoute

VPN type ⓘ

Route-basedPolicy-based

* SKU ⓘ

Basic

▼

* Virtual network ⓘ

Choose a virtual network

>

To associate a virtual network with a gateway, it must contain a valid gateway subnet.
[Learn more](#)

These are the virtual networks in the selected subscription and location 'Southeast Asia'.

SonicWall-Azure-Site2-Site-...
SonicWall-Azure-Site2-...

Site-2-Site-VPN-SonicWall
Site-2-Site-VPN-Sonic...

ⓘ

* Virtual network ⓘ
SonicWall-Azure-Site2-Site-VPN-... >

* Gateway subnet address range ⓘ
10.2.0.0/24 ✓
10.2.0.0 - 10.2.0.255 (256 addresses)

* Public IP address ⓘ
Choose a public IP address >

* Subscription
Azure in Open ▼

Resource group ⓘ
SonicWall-Azure-Site2-Site-VPN-LAB

* Location ⓘ
Southeast Asia ▼

☐ Pin to dashboard

[Create](#) [Automation options](#)

Provisioning a virtual network gateway may take up to 45 minutes.

Creating Public IP Address

Give some identical name to your Public IP Address as per your environment.

Create public IP address

*

Name

VNG-4-SonicWall-VPN

OK

Define Gateway Subnet

Create virtual network gate... □ ×

Route-basedPolicy-based

* SKU ⓘ

Basic

* Virtual network ⓘ

SonicWall-Azure-Site2-Site-VPN-...

* Gateway subnet address range ⓘ

10.2.0.0/24

10.2.0.0 - 10.2.0.255 (256 addresses)

* Public IP address ⓘ

(new) VNG-4-SonicWall-VPN

* Subscription

Azure in Open

Resource group ⓘ

SonicWall-Azure-Site2-Site-VPN-LAB

* Location ⓘ

Southeast Asia

☐ Pin to dashboard

Create

Automation options

Provisioning a virtual network gateway may take up to 45 minutes.

Click on create and as its saying it will take approximately 45 minute to create Virtual Network Gateway.

At notification area, you can see the progress and status of Virtual Network Creation.

Notifications



Dismiss: Informational Completed [All](#)

■■■ Deployment in progress... Running

Deployment to resource group 'SonicWall-Azure-Site2-Site-VPN-LAB' is in progress.

Dashboard Status of Virtual Network Gateway

At this point you can view the status of virtual Network Gateway creation, usually it takes 20 to 35 minutes but its depend datacenter to datacenter. By default, Gateway message will intimate about 45 minutes' creation time.

The screenshot shows the Azure Dashboard interface. The top navigation bar includes the 'Dashboard' title, a dropdown arrow, and links for '+ New dashboard', 'Edit dashboard', 'Share', 'Fullscreen', 'Clone', and 'Delete'. The main content area is divided into several sections. On the left, under 'Quickstart tutorials', there are links for 'Windows Virtual Machines', 'Linux Virtual Machines', 'App Service', and 'Functions'. On the right, the 'Azure Health MY RESOURCES' section displays a world map with green checkmarks indicating resource health. Below this, the 'SonicWall-Azure-Site...' resource is highlighted, showing a blue square icon with a white dot. A red box highlights the text 'Deploying Virtual network gateway' next to the icon.

Dashboard
+ New dashboard
Edit dashboard
Share
Fullscreen
Clone
Delete

Quickstart tutorials

Windows Virtual Machines
Provision Windows Server, SQL Server, SharePoint VMs

Linux Virtual Machines
Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs

App Service
Create Web Apps using .NET, Java, Node.js, Python, PHP

Functions
Process events with a serverless code architecture

Azure Health
MY RESOURCES

SonicWall-Azure-Site...

VNG-4-SonicWall-VPN

Property of Virtual Network Gateway

Click on VNG-4-SonicWall-VPN you will see the Gateway properties having information about public IP address and VPN properties.

Move Delete	
Essentials ^	
Resource group (change)	
SonicWall-Azure-Site2-Site-VPN-LAB	
Location	
Southeast Asia	
Subscription name (change)	
Azure in Open	
Subscription ID	
bdba14a	36d9d
SKU	Basic
Gateway type	VPN
VPN type	Route-based
Virtual network	SonicWall-Azure-Site2-Site-VPN-LAB
Public IP address	52. (VNG-4-SonicWall-VPN)

You can see the Virtual Network Gateway assign a public address which is starting from 52.

Let do the connectivity parameter from Azure end.

Click on Virtual Network Gateway you have just created.

Insides of Virtual Network Gateway

At this point you can see the properties of the VNG

Microsoft Azure VNG-4-SonicWall-VPN - Connections

VNG-4-SonicWall-VPN - Connections
Virtual network gateway

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- SETTINGS
 - Configuration
 - Connections
 - Point-to-site configuration
 - Properties
 - Locks
 - Automation script
- SUPPORT + TROUBLESHOOTING
 - Resource health
 - Reset

+ Add

Search connections

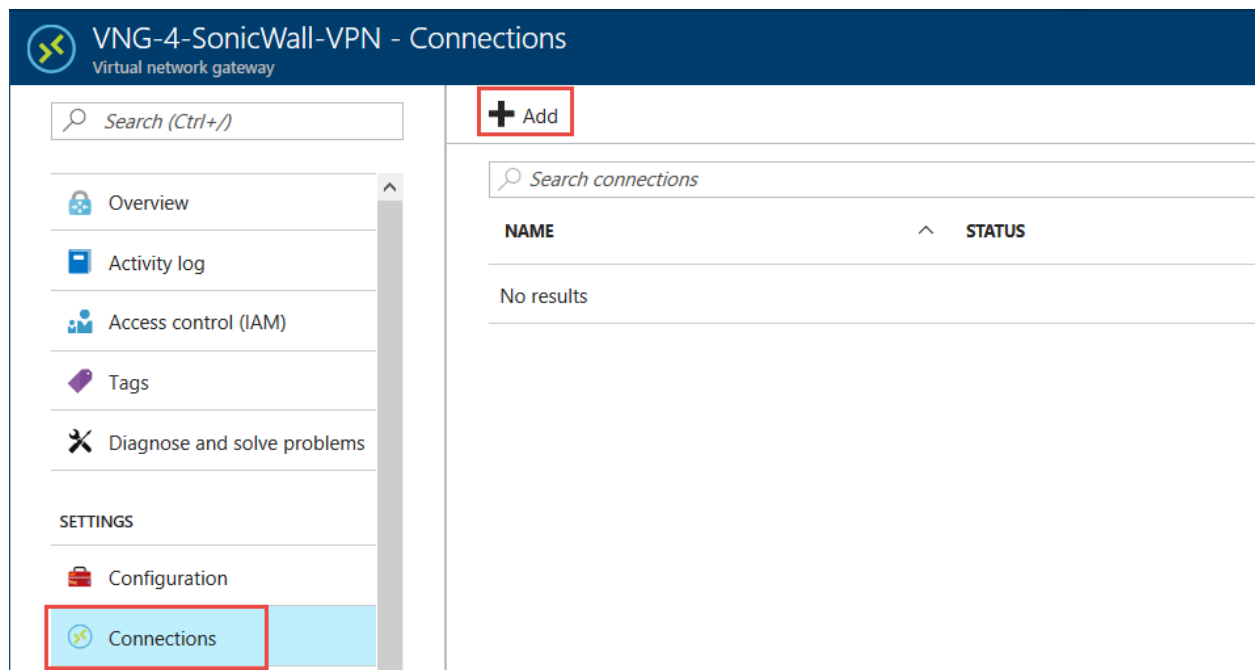
NAME	STATUS
No results	

These are different properties of the VNG created for SonicWall site to site VPN, you can explore different options available here.

Click on connection you will see that there is no connection available right now.

Creating Connection Under Virtual Network Gateway

Let's create connection under VNG.



Click on Connection and then Click on +Add

NAME	STATUS	CONNECTION TYPE	PEER
Connection-With-SonicWall-VPN-LAB	Unknown	Site-to-site (IPsec)	SonicWall-Side-Network

At this point we created connection in which we define pre-shared key and SonicWall Side Network

You can see that status of the connection is showing as unknow because we have not yet configured the SonicWall side VPN connection.

Creating an Address Object for the virtual network

To create an Address Object:

- 1 Navigate to the Network > Address Objects dialog.
- 2 Click Add to create a new Address Object.

SONICWALL | Network Security Appliance

Name: AzureVPN

Zone Assignment: VPN

Type: Network

Network: 10.2.2.0

Netmask/Prefix Length: 255.255.255.0

Ready

OK Cancel

Enter the following information:

Name – Enter a name for the Address Object (Azure Network is used in this example)

Zone Assignment – Click the drop-down, and then select VPN.

Type – Click the drop-down, and then select Network.

Network – Enter the network IP address as shown in the SonicWall-Azure-Site2-Site-VPN-LAB - Subnets Quick Start dialog.

Netmask/Prefix Length – Enter the netmask.

Click Add.

SonicWall VPN Connection Creation

To create a policy-based VPN on the firewall:

1. Log into the SonicOS management interface as an administrator.
2. Navigate to the VPN > Settings dialog.
3. Click Add.

1. Policy Type—Select Site to Site from the drop-down menu.
2. Authentication Method—Select the IKE using Preshared Secret authentication method.
3. Name—Enter a name for the policy (this example uses Azure).
4. IPsec Primary Gateway Name or Address—Enter the AZURE GATEWAY IP ADDRESS displayed on the Virtual Network VNG-4-SonicWall-VPN Dashboard

dialog of the Azure Management Portal. Refer to the Creating a Virtual Network Gateway section.

5. Shared Secret – This is auto-generated by Azure. Copy it from the Azure Virtual Network dashboard, under Manage Key, and then enter it into this field. For more information, see Managing Shared Keys.
6. Click the Network tab.
7. Click the Choose local network from list option, and then select the desired local network. (This could vary depending on your network. The X0 Subnet is used in this example.)

NOTE: This needs to be the same local network that was previously entered in the Azure Management Portal under the Starting IP text-field. Refer to Defining the SonicWALL Network to obtain this IP address.

Select Choose destination network from list.

General

Network

Proposals

Advanced

Local Networks☒ Choose local network from list

X16:V18 Subnet

☐ Any address**Remote Networks**☐ Use this VPN Tunnel as default route for all Internet traffic☒ Choose destination network from list

AzureVPN

☐ Use IKEv2 IP Pool

--Select IP Pool Network--



Ready

OK

Cancel

Help

Here I have selected my VLAN 16 and 18, I have already defined both Vlan subnets at Azure management portal.

Remote Network is the Object we have just created above, this is Azure side network.

Click the Proposals tab.

Select the Exchange > Main Mode.

Azure supports only Main Mode for static-routing site to site VPN. For more information about the Proposals supported in Azure.

General

Network

Proposals

Advanced

IKE (Phase 1) Proposal

Exchange:	IKEv2 Mode ▼
DH Group:	Group 2 ▼
Encryption:	AES-256 ▼
Authentication:	SHA1 ▼
Life Time (seconds):	28800

Ipssec (Phase 2) Proposal

Protocol:	ESP ▼
Encryption:	AES-256 ▼
Authentication:	SHA1 ▼
<input type="checkbox"/> Enable Perfect Forward Secrecy	
Life Time (seconds):	28800

Ready

OK

Cancel

Help

Click the Advanced tab.

Advanced Settings

☒ Enable Keep Alive

☐ Suppress automatic Access Rules creation for VPN Policy

☐ Disable IPsec Anti-Replay

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

WXA Group: None

☐ Display Suite B Compliant Algorithms Only

☐ Apply NAT Policies

☐ Allow SonicPointN Layer 3 Management

Management via this SA: ☐ HTTPS ☐ SSH ☐ SNMP

User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional): 0.0.0.0

VPN Policy bound to: Interface X1

IKEv2 Settings

☒ Do not send trigger packet during IKE SA negotiation

☐ Accent Hash & URI Certificate Type

Ready

OK Cancel Help

Check Enable Keep Alive to use heartbeat messages between peers on this VPN tunnel.

If one end of the tunnel fails, using Keep Alives allows the automatic renegotiation of the tunnel without having to wait for the proposed Life Time to expire.

For the VPN Policy bound to field, select the appropriate interface from the drop-down list (the WAN interface on the SonicWALL firewall).

Click OK.

Testing the connectivity

The SonicWALL firewall automatically initiates the VPN connection and keeps it alive when Keep Alive is enabled.

	3	Azure-Site-2-Site-With-SonicWall	52.		10.2.2.0 - 10.2.2.255	ESP: AES-256/HMAC SHA1 (IKEv2)			
Add...		Delete		Delete All					

To test the connectivity from Azure:

Go to the Azure Management Portal, and navigate to Virtual Networks Gateway.

Click the Connection and go to its Dashboard.

You can see the connection status changed from unknown to Connected.

VNG-4-SonicWall-VPN - Connections				
Virtual network gateway				
Search (Ctrl+/)				
+ Add				
Search connections				
NAME	STATUS	CONNECTION TYPE	PEER	
Connection-With-SonicWall-VPN-LAB	Connected	Site-to-site (IPsec)	SonicWall-Side-Network	...

Click on the connected connection to view its property.

Connection-With-SonicWall-VPN-LAB		
Connection		
Search (Ctrl+/)		
Overview		
Activity log		
Access control (IAM)		
Tags		
Diagnose and solve problems		
SETTINGS		
Configuration		
Connections		
Move Delete		
Essentials		
Resource group (change)		
SonicWall-Azure-Site2-Site-VPN-LAB		
Status		
Connected		
Location		
Southeast Asia		
Subscription name (change)		
Azure in Open		
Subscription ID		
bdba14: 36d9d		
Data in		
0 B		
Data out		
0 B		
Virtual network		
SonicWall-Azure-Site2-Site-VPN-LAB		
Virtual network gateway		
VNG-4-SonicWall-VPN (52.)		
Local network gateway		
SonicWall-Side-Network (2.)		

We have successfully configured Azure Site to Site VPN with SonicWall hardware Firewall.

Now you can create Virtual Machines in Azure and can access Azure VMs from your Network.

In next lab, I will show you how you can configure Point to Site VPN with Azure and how to configure Site to Site VPN with Windows Server 2012 R2.